NETWORK WORKING GROUP
Internet-Draft
Intended status: Informational
Expires: October 30, 2015

J. Hall
CDT
M. Aaron
CU Boulder
B. Jones
GA Tech

April 28, 2015

A Survey of Worldwide Censorship Techniques
draft-hall-censorship-tech-01

Abstract

This document describes the technical mechanisms used by censorship regimes around the world to block or degrade internet traffic. It aims to make designers, implementers, and users of Internet protocols aware of the properties being exploited and mechanisms used to censor end-user access to information. This document makes no suggestions on individual protocol considerations, and is purely informational, intended to be a reference.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document describes the technical mechanisms used by censorship regimes around the world to block or degrade internet traffic. To that end, we describe three elements of Internet censorship: aggregation, identification, and prevention. Aggregation is the process by which censors determine what they should block, i.e. they decide to block a list of pornographic websites. Identification is the process by which censors determine whether content is blocked, i.e. the censor blocks all webpages containing "sex" in the title. Prevention is the process by which the censor intercedes in communication and prevents access to censored materials.

2. Technical Aggregation

Aggregation is the process of figuring out what censors would like to block. Generally, censors aggregate "to block" information in three possible sorts of blacklists: Keyword, Domain Name, or IP. Keyword and Domain Name blocking take place at the application level (e.g. HTTP), whereas IP blocking tends to take place in the TCP/IP header. The mechanisms for building up these blacklists are varied. Many times private industries that sell "content control" software, such as SmartFilter, provide their services to nations which can then pick from broad categories, such as gambling or pornography, that they would like to block [1]. In these cases, the private services embark on an attempt to label every semi-questionable website as to allow for this metatag blocking. Countries that are more interested in retaining specific political control, a desire which requires swift and decisive action, often have ministries or organizations, such as the Ministry of Industry and Information Technology in China or the Ministry of Culture and Islamic Guidance in Iran, which maintain their own blacklists.

3. Technical Identification

3.1. Points of Control

Digital censorship, necessarily, takes place over a network. Network design gives censors a number of different points-of-control where they can identify the content they are interested in filtering. An important aspect of pervasive technical interception is the necessity to rely on software or hardware to intercept the content the censor is interested in. This requirement, the need to have the interception mechanism located somewhere, logically or physically, implicates four general points-of-control:

- Internet Backbone: If a censor controls the gateways into a region, they can filter undesirable traffic that is traveling into and out of the region by sniffing and mirroring at the relevant exchange points. Censorship at this point-of-control is most effective at controlling the flow of information between a region and the rest of the internet, but is ineffective at identifying content traveling between the users within a region.

- Internet Service Providers: Internet Service Providers are perhaps the most natural point-of-control. They have a benefit of being easily enumerable by a censor paired with the ability to identify the regional and international traffic of all their users. The censor's filtration mechanisms can be placed on an ISP via governmental mandates, ownership, or voluntary/coercive influence.

- Institutions: Private institutions such as corporations, schools, and cyber cafes can put filtration mechanisms in place. These mechanisms are occasionally at the request of a censor, but are more often implemented to help achieve institutional goals, such as to prevent the viewing of pornography on school computers.

- Personal Devices: Censors can mandate censorship software be installed on the device level. This has many disadvantages in terms of scalability, ease-of-circumvention, and operating system requirements. The emergence of mobile devices exacerbate these feasibility problems.

At all levels of the network hierarchy, the filtration mechanisms used to detect undesirable traffic are essentially the same: a censor sniffs transmitting packets and identifies undesirable content, and then uses a blocking or shaping mechanism to prevent or degrade access. Identification of undesirable traffic can occur at the application, transport, or network layer of the IP stack. Censors are almost always concerned with web traffic, so the relevant protocols tend to be filtered in predictable ways. For example, a

subversive image would always make it past a keyword filter, but the IP address of the site serving the image may be blacklisted when identified as a provider of undesirable content.

3.2. Application Layer

3.2.1. HTTP Request Header Identification

An HTTP header contains a lot of useful information for traffic identification; although host is the only required field in an HTTP request header, an HTTP method field is necessary to do anything useful. As such, the method and host fields are the two fields used most often for ubiquitous censorship. A censor can sniff traffic and identify a specific domain name (host) and usually a page name (GET /page) as well. This identification technique is usually paired with TCP/IP header identification (see Section 3.3.1) for a more robust method.

Tradeoffs: Request Identification is a technically straight-forward identification method that can be easily implemented at the Backbone or ISP level. The hardware needed for this sort of identification is cheap and easy-to-acquire, making it desirable when budget and scope are a concern. HTTPS will encrypt the relevant request and response fields, so pairing with TCP/IP identification (see Section 3.3.1) is necessary for filtering of HTTPS.

Empirical Examples: Studies exploring censorship mechanisms have found evidence of HTTP header/ URL filtering in many countries, including Bangladesh, Bahrain, China, India, Iran, Malaysia, Pakistan, Russia, Saudi Arabia, South Korea, Thailand, and Turkey [58][59][60]. Commercial technologies such as the McAfee SmartFilter and NetSweeper are often purchased by censors [2]. These commercial technologies use a combination of HTTP Request Identification and TCP/IP Header Identification to filter specific URLs. Dalek et al. and Jones et al. identified the use of these products in the wild [2][61].

3.2.2. HTTP Response Header Identification

While HTTP Request Header Identification relies on the information contained in the HTTP request from client to server, response identification uses information sent in response by the server to client to identify undesirable content.

Tradeoffs: As with HTTP Request Header Identification, the techniques used to identify HTTP traffic are well-known, cheap, and relatively easy to implement, but is made useless by HTTPS, because the response in HTTPS is encrypted, including headers.

The response fields are also less helpful for identifying content than request fields, as Server could easily be identified using HTTP Request Header identification, and Via is rarely relevant. HTTP Response censorship mechanisms normally let the first n packets through while the mirrored traffic is being processed; this may allow some content through and the user may be able to detect that the censor is actively interfering with undesirable content.

Empirical Examples: In 2009, Jong Park et al. at the University of New Mexico demonstrated that the Great Firewall of China (GFW) used this technique [3]. However, Jong Park et al. found that the GFW discontinued this practice during the course of the study. Due to the overlap in HTTP response filtering and keyword filtering (see Section 3.2.3), it is likely that most censors rely on keyword filtering over TCP streams instead of HTTP response filtering.

3.2.3. Instrumenting Content Providers

In addition to censorship by the state, many governments pressure content providers to censor themselves. Due to the extensive reach of government censorship, we need to define content provider as any service that provides utility to users, including everything from web sites to locally installed programs. The defining factor of keyword identification by content providers is the choice of content providers to detect restricted terms on their platform. The terms to look for may be provided by the government or the content provider may be expected to come up with their own list.

Tradeoffs: By instrumenting content providers to identify restricted content, the censor can gain new information at the cost of political capital with the companies it forces or encourages to participate in censorship. For example, the censor can gain insight about the content of encrypted traffic by coercing web sites to identify restricted content, but this may drive away potential investment. Coercing content providers may encourage self censorship, an additional advantage for censors. The tradeoffs for instrumenting content providers are highly dependent on the content provider and the requested assistance.

Empirical Examples: Researchers have discovered keyword identification by content providers on platforms ranging from instant messaging applications [63] to search engines [62][4][6][7][8]. To demonstrate the prevalence of this type of keyword identification, we look to search engine censorship.

Search engine censorship demonstrates keyword identification by content providers and can be regional or worldwide. Implementation is occasionally voluntary, but normally is based on laws and

regulations of the country a search engine is operating in. The keyword blacklists are most likely maintained by the search engine provider. China requires search engine providers to "voluntarily" maintain search term blacklists to acquire/keep an Internet content provider (ICP) license [4]. It is clear these blacklists are maintained by each search engine provider based on the slight variations in the intercepted searches [5][6]. The United Kingdom has been pushing search engines to self censor with the threat of litigation if they don't do it themselves: Google and Microsoft have agreed to block more than 100,00 queries in U.K. to help combat abuse [7][8].

Depending on the output, search engine keyword identification may be difficult or easy to detect. In some cases specialized or blank results provide a trivial enumeration mechanism, but more subtle censorship can be difficult to detect. In February, Microsoft's search engine, Bing, was accussed of censoring Chinese content outside of China [62] because Bing returned different results for censored terms in Chinese and English. However, it is possible that censorship of the largest base of Chinese search users, China, biased Bing's results so that the more popular results in China (the uncensored results) were also more popular for Chinese speakers outside of China.

3.2.4. Deep Packet Inspection (DPI) Identification

Deep Packet Inspection has become computationally feasible as a censorship mechanism in the past 5 years [9]. Unlike other techniques, DPI reassembles network flows to examine the application "data" section, as opposed to only the header, and is therefore often used for keyword identification. DPI also differs from other identification technologies because it can leverage additional packet and flow characteristics, i.e. packet sizes and timings, to identify content. To prevent substantial quality of service (QoS) impacts, DPI normally analyzes a copy of data while the original packets continue to be routed. Typically, the traffic is split using either a mirror switch or fiber splitter, and analyzed on a cluster of machines running Intrusion Detection Systems (IDS) configured for censorship.

Tradeoffs: DPI is one of the most expensive identification mechanisms and can have a large QoS impact [10]. When used as a keyword filter for TCP flows, DPI systems can cause also major overblocking problems. Like other techniques, DPI is less useful against encrypted data, though DPI can leverage unencrypted elements of an encrypted data flow (e.g., the Server Name Indicator (SNI) sent in the clear for TLS) or statistical information about an encrypted flow (e.g., video takes more bandwidth than audio or textual forms of

communication) to identify traffic.

Despite these problems, DPI is the most powerful identification method and is widely used in practice. The Great Firewall of China (GFW), the largest censorship system in the world, uses DPI to identify restricted content over HTTP and DNS and inject TCP RSTs and bad DNS responses, respectively, into connections [3][64][65].

Empirical Evidence: Several studies have found evidence of DPI being used to censor content and tools. Clayton et al. Crandal et al., Anonymous, and Khattak et al., all explored the GFW and Khattak et al. even probed the firewall to discover implementation details like how much state it stores [3][64][65][66]. The Tor project claims that China, Iran, Ethiopia, and others must being using DPI to block the obsf2 protocol [11]. Malaysia has been accused of using targeted DPI, paired with DDoS, to identify and subsequently knockout pro-opposition material [12]. It also seems likely that organizations not so worried about blocking content in real-time could use DPI to sort and categorically search gathered traffic using technologies such as NarusInsight [13].

3.3. Transport Layer

3.3.1. TCP/IP Header Identification

TCP/IP Header Identification is the most pervasive, reliable, and predictable type of identification. TCP/IP headers contain a few invaluable pieces of information that must be transparent for traffic to be successfully routed: destination and source IP address and port. Destination and Source IP are doubly useful, as not only does it allow a censor to block undesirable content via IP blacklisting, but also allows a censor to identify the IP of the user making the request. Port is useful for whitelisting certain applications.

Trade-offs: TCP/IP identification is popular due to its simplicity, availability, and robustness.

TCP/IP identification is trivial to implement, but is difficult to implement in backbone or ISP routers at scale, and is therefore typically implemented with DPI. Blacklisting an IP is equivalent to installing a /32 route on a router and due to limited flow table space, this cannot scale beyond a few thousand IPs at most. IP blocking is also relatively crude, leading to overblocking, and cannot deal with some services like Content Distribution Networks (CDN), that host content at hundreds or thousands of IP addresses. Despite these limitations, IP blocking is extremely effective because the user needs to proxy their traffic through another destination to circumvent this type of identification.

Port-blocking is generally not useful because many types of content share the same port and it is possible for censored applications to change their port. For example, most HTTP traffic goes over port 80, so the censor cannot differentiate between restricted and allowed content solely on the basis of port. Port whitelisting is occasionally used, where a censor limits communication to approved ports, such as 80 for HTTP traffic and is most effective when used in conjuction with other identification mechanisms. For example, a censor could block the default HTTPS port, port 443, thereby forcing most users to fall back to HTTP.

3.3.2. Protocol Identification

Censors sometimes identify entire protocols to be blocked using a variety of traffic characteristics. For example, Iran degrades the performance of HTTPS traffic, a procotol that prevents further analysis, to encourage users to switch to HTTP, a protocol that they can analyze [60]. A simple protocol identification would be to recognize all TCP traffic over port 443 as HTTPS, but more sophisticated analysis of the statistical properties of payload data and flow behavior, would be more effective, even when port 443 is not used [14][15].

If censors can detect circumvention tools, they can block them, so censors like China are extremely interested in identifying the protocols for censorship circumvention tools. In recent years, this has devolved into an arms race between censors and circumvention tool developers. As part of this arms race, China developed an extremely effective protocol identification technique that researchers call active probing or active scanning.

In active probing, the censor determines whether hosts are running a circumvention protocol by trying to initiate communication using the circumvention protocol. If the host and the censor successfully negotiate a connection, then the censor conclusively knows that host is running a circumvention tool. China has used active scanning to great effect to block Tor [17].

Trade-offs: Protocol Identification necessarily only provides insight into the way information is traveling, and not the information itself.

Protocol identification is useful for detecting and blocking circumvention tools, like Tor, or traffic that is difficult to analyze, like VoIP or SSL, because the censor can assume that this traffic should be blocked. However, this can lead to overblocking problems when used with popular protocols. These methods are expensive, both computationally and financially, due to the use of

statistical analysis, and can be ineffective due to its imprecise nature.

Empirical Examples: Protocol identification can be easy to detect if it is conducted in real time and only a particular protocol is blocked, but some types of protocol identification, like active scanning, are much more difficult to detect. Protocol identification has been used by Iran to identify and throttle SSH traffic to make it unusable [16] and by China to identify and block Tor relays [17]. Protocol Identification has also been used for traffic management, such as the 2007 case where Comcast in the United States used RST injection to interrupt BitTorrent Traffic [17].

4. Technical Prevention

4.1. Packet Dropping

Packet dropping is a simple mechanism to prevent undesirable traffic. The censor identifies undesirable traffic and chooses to not properly forward any packets it sees associated with the traversing undesirable traffic instead of following a normal routing protocol. This can be paired with any of the previously described mechanisms so long as the censor knows the user must route traffic through a controlled router.

Trade offs: Packet Dropping is most successful when every traversing packet has transparent information linked to undesirable content, such as a Destination IP. One downside Packet Dropping suffers from is the necessity of overblocking all content from otherwise allowable IP's based on a single subversive sub-domain; blogging services and github repositories are good examples. China famously dropped all github packets for three days based on a single repository hosting undesirable content [18]. The need to inspect every traversing packet in close to real time also makes Packet Dropping somewhat challenging from a QoS perspective.

Empirical Examples: Packet Dropping is a very common form of technical prevention and lends itself to accurate detection given the unique nature of the time-out requests it leaves in its wake. The Great Firewall of China uses packet dropping as one of its primary mechanisms of technical censorship [19]. Iran also uses Packet Dropping as the mechanisms for throttling SSH [20]. These are but two examples of a ubiquitous censorship practice.

4.2. RST Packet Injection

Packet injection, generally, refers to a man-in-the-middle (MITM) network interference technique that spoofs packets in an established traffic stream. RST packets are normally used to let one side of TCP connection know the other side has stopped sending information, and thus the receiver should close the connection. RST Packet Injection is a specific type of packet injection attack that is used to interrupt an established stream by sending RST packets to both sides of a TCP connection; as each receiver thinks the other has dropped the connection, the session is terminated.

Trade-offs: RST Packet Injection has a few advantages that make it extremely popular is a censorship technique. RST Packet Injection is an out-of-band prevention mechanism, allowing the avoidance of the the QoS bottleneck one can encounter with inline techniques such as Packet Dropping. This out-of-band property allows a censor to

inspect a copy of the information, usually mirrored by an optical splitter, making it an ideal pairing for DPI and Protocol Identification [21]. RST Packet Injection also has the advantage of only requiring one of the two endpoints to accept the spoofed packet for the connection to be interrupted [22]. The difficult part of RST Packet Injection is spoofing "enough" correct information to ensure one end-point accepts a RST packet as legitimate; this generally implies a correct IP, port, and (TCP) sequence number. Sequence number is the hardest to get correct, as RFC 793 specifies an RST Packet should be in-sequence to be accepted, although the RFC also recommends allowing in-window packets as "good enough" [23]. This in-window recommendation is important, as if it is implement it allows for successful Blind RST Injection attacks [24]. When in-window sequencing is allowed, It is trivial to conduct a Blind RST Injection, a blind injection implies the censor doesn't know any sensitive (encrypted) sequencing information about the TCP stream they are injecting into, they can simply enumerate the ~70000 possible windows; this is particularly useful for interrupting encrypted/obfuscated protocols such as SSH or Tor. RST Packet Injection relies on a stateful network, making it useless against UDP connections. RST Packet Injection is among the most popular censorship techniques used today given its versatile nature and effectiveness against all types of TCP traffic.

Empirical Examples: RST Packet Injection, as mentioned above, is most often paired with identification techniques that require splitting, such as DPI or Protocol Identification. In 2007 Comcast was accused of using RST Packet Injection to interrupt traffic it identified as BitTorrent [25], this later led to a US Fderal Communications Commission ruling against Comcast [26]. China has also been known to use RST Packet Injection for censorship purposes. This prevention is especially evident in the interruption of encrypted/obfuscated protocols, such as those used by Tor [27].

4.3. DNS Cache Poisoning

DNS Cache Poisoning refers to a mechanism where a censor interferes with the response sent by a DNS resolver to the requesting device by injecting an alternative IP address into the response message on the return path. Cache poisoning occurs after the requested site's name servers resolve the request and attempt to forward the IP back to the requesting device; on the return route the resolved IP is recursively cached by each DNS server that initially forwarded the request. During this caching process if an undesirable keyword is recognized, the resolved IP is poisoned and an alternative IP is returned. These alternative IP's usually direct to a nonsense domain or a warning page [28]. Alternatively, Iranian censorship appears to prevent the communication en-route, preventing a response from ever being sent

[29].

Trade-offs: DNS Cache Poisoning is one of the rarer forms of prevention due to a number of shortcomings. DNS Cache Poisoning requires the censor to force a user to traverse a controlled DNS resolver for the mechanism to be effective, it is easily circumvented by a technical savvy user that opts to use alternative DNS resolvers, such as the 8.8.8.8/8.8.4.4 public DNS resolvers provided by Google. DNS Cache Poisoning also implies returning an incorrect IP to those attempting to resolve a domain name, but the site is still technically unblocked if the user has another method to acquire the IP address of the desired site. Blocking overflow has also been a problem, as occasionally users outside of the censors region will be directed through a DNS server controlled by a censor, causing the request to fail. The ease of circumvention paired with the large risk of overblocking and blocking overflow make DNS Cache Poisoning a partial, difficult, and less than ideal censorship mechanism.

Empirical Evidence: DNS Cache Poisoning, when properly implemented, is easy to identify based on the shortcomings identified above. Turkey relied on DNS Cache Poisoning for its country-wide block of websites such Twitter and Youtube for almost week in March of 2014 but the ease of circumvention resulted in an increase in the popularity of Twitter until Turkish ISP's implementing an IP blacklist to achieve the governmental mandate [30]. To drive proverbial "nail in the coffin" Turkish ISPs started hijacking all requests to Google and Level 3's international DNS resolvers [31]. DNS Cache Poisoning, when incorrectly implemented, has as has resulted in some of the largest "censorship disasters". In January 2014 China started directing all requests passing through the Great Fire Wall to a single domain, dongtaiwang.com, due to an improperly configured DNS Cache Poisoning attempt; this incident is thought to be the largest internet-service outage in history [32][33]. Countries such as China, Iran, Turkey, and the United States have discussed blocking entire TLDs as well, but only Iran has acted by blocking all Israeli (.il) domains [34].

4.4. Distributed Denial of Service (DDoS)

Distributed Denial of Service attacks are a common attack mechanism used by "hacktivists" and black-hat hackers, but censors have used DDoS in the past for a variety of reasons. There is a huge variety of DDoS attacks [35], but on a high level two possible impacts tend to occur; a flood attack results in the service being unusable while resources are being spent to flood the service, a crash attack aims to crash the service so resources can be reallocated elsewhere without "releasing" the service.

Trade-offs: DDoS is an appealing mechanism when a censor would like to prevent all access to undesirable content, instead of only access in their region for a limited period of time, but this is really the only uniquely beneficial feature for DDoS as a censorship technique. The resources required to carry out a successful DDoS against major targets are computationally expensive, usually requiring renting or owning a malicious distributed platform such as a botnet, and imprecise. DDoS is an incredibly crude censorship technique, and appears to largely be used as a timely, easy-to-access mechanism for blocking undesirable content for a limited period of time.

Empirical Examples: In 2012 the U.K.'s GCHQ used DDoS to temporarily shutdown IRC chat rooms frequented by members of Anonymous using the Syn Flood DDoS method; Syn Flood exploits the handshake used by TCP to overload the victim server with so many requests that legitimate traffic becomes slow or impossible [36][37]. Dissenting opinion websites are frequently victims of DDoS around politically sensitive events in Burma [38]. Controlling parties in Russia [39], Zimbabwe [40], and Malaysia [41] have been accused of using DDoS to interrupt opposition support and access during elections.

4.5. Network Disconnection or Adversarial Route Announcement

While it is perhaps the crudest of all censorship techniques, there is no more effective way of making sure undesirable information isn't allowed to propagate on the web than by shutting off the network. The network can be logically cut off in a region when a censoring body withdraws all of the Boarder Gateway Protocol (BGP) prefixes routing through the censor's country.

Trade-offs: The impact to a network disconnection in a region is huge and absolute; the censor pays for absolute control over digital information with all the benefits the internet brings; this is never a long-term solution for any rational censor and is normally only used as a last resort in times of substantial unrest.

Empirical Examples: Network Disconnections tend to only happen in times of substantial unrest, largely due to the huge social, political, and economic impact such a move has. One of the first, highly covered occurrences was with the Junta in Myanmar employing Network Disconnection to help Junta forces quash a rebellion in 2007 [42]. China disconnected the network in the Xinjiang region during unrest in 2009 in an effort to prevent the protests from spreading to other regions [43]. The Arab Spring saw the the most frequent usage of Network Disconnection, with events in Egypt and Libya in 2011 [44][45], and Syria in 2012 [46].

5. Non-Technical Aggregation

As the name implies, sometimes manpower is the easiest way to figure out which content to block. Manual Filtering differs from the common tactic of building up blacklists in that is doesn't necessarily target a specific IP or DNS, but instead removes or flags content. Given the imprecise nature of automatic filtering, manually sorting through content and flagging dissenting websites, blogs, articles and other media for filtration can be an effective technique. This filtration can occur on the Backbone/ISP level, China's army of monitors is a good example [47]; more commonly manual filtering occurs on an institutional level. (Internet Content Provider?) ICP's, such as Google or Weibo, require a business license to operate in China. One of the prerequisites for a business license is an agreement to sign a "voluntary pledge" known as the "Public Pledge on Self-discipline for the Chinese Internet Industry". The failure to " energetically uphold" the pledged values can lead to the ICP's being held liable for the offending content by the Chinese government [47].

6. Non-Technical Prevention

6.1. Self Censorship

Self censorship is one of the most interesting and effective types of censorship; a mix of Bentham's Panopticon, cultural manipulation, intelligence gathering, and meatspace enforcement. Simply put, self censorship is when a censor creates an atmosphere where users censor themselves. This can be achieved through controlling information, intimidating would-be dissidents, swaying public thought, and creating apathy. Self censorship is difficult to document, as when it is implemented effectively the only noticeable tracing is a lack of undesirable content; instead one must look at the tools and techniques used by censors to encourage self-censorship. Controlling Information relies on traditional censorship techniques, or by forcing all users to connect through an intranet, such as in North Korea. Intimidation is often achieved through allowing internet users to post "whatever they want", but arresting those who post about dissenting views, this technique is incredibly common [48][49][50][51][52]. A good example of swaying public thought is China's "50-Cent Party", composed of somewhere between 20,000 [53] and 300,000 [54] contributors who are paid to "guide public thought" on local and regional issues as directed by the Ministry of Culture. Creating apathy can be a side-effect of successfully controlling information over time and is ideal for a censorship regime [55].

6.2. Domain Name Reallocation

As Domain Names are resolved recursively, if a TLD deregisters a domain all other DNS resolvers will be unable to properly forward and cache the site. Domain name registration is only really a risk where undesirable content is hosted on TLD controlled by the censoring country, such as .ch or .ru [56].

6.3. Server Takedown

Servers must have a physical location somewhere in the world. If undesirable content is hosted in the censoring country the servers can be physically seized or the hosting provider can be required to prevent access [57].

7. References

[1] Glanville, J., "The Big Business of Net Censorship", November 2008, <http://www.theguardian.com/commentisfree/2008/nov/17/censorship-internet>.

[2] Dalek, J., "A Method for Identifying and Confirming the Use of URL Filtering Products for Censorship", October 2013 , <http://www.cs.stonybrook.edu/~phillipa/papers/imc112s-dalek.pdf>.

[3] Crandall, J., "Empirical Study of a National-Scale Distributed Intrusion Detection System: Backbone-Level Filtering of HTML Responses in China"", June 2010 , <http://www.cs.unm.edu/~crandall/icdcs2010.pdf >.

[4] Cheng, J., "Google stops Hong Kong auto-redirect as China plays hardball"", June 2010, <http://arstechnica.com/tech-policy/2010/06/google-tweaks-china-to-hong-kong-redirect-same-results/>.

[5] Zhu, T., "An Analysis of Chinese Search Engine Filtering"", July 2011 , <http://arxiv.org/ftp/arxiv/papers/1107/1107.3794.pdf#page=10>.

[6] Whittaker, Z., "1,168 keywords Skype uses to censor, monitor its Chinese users", March 2013 , <http://www.zdnet.com/1168-keywords-skype-uses-to-censor-monitor-its-chinese-users-7000012328/>.

[7] News, B., "Google and Microsoft agree steps to block abuse images", November 2013 , <http://www.bbc.com/news/uk-24980765>.

[8] Condliffe, J., "Google Announces Massive New Restrictions on Child Abuse Search Terms", November 2013 , <http://gizmodo.com/google-announces-massive-new-restrictions-on-child-abus-1466539163>.

[9] Wagner, B., "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'", June 2009 , <http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf>.

[10] Porter, T., "The Perils of Deep Packet Inspection", Oct 2010, < http://www.symantec.com/connect/articles/perils-deep-packet-inspection>.

[11] Wilde, T., "Knock Knock Knockin' on Bridges Doors",

January 2012, <https://blog.torproject.org/blog/knock-knock-knockin-bridges-doors>.

[12] Wagstaff, J., "In Malaysia, online election battles take a nasty turn", May 2013, <http://www.reuters.com/article/2013/05/04/uk-malaysia-election-online-idUKBRE94309G20130504>.

[13] EFF, T., "Hepting vs. ATand T", Updated December, <https://www.eff.org/cases/hepting>.

[14] Hjelmvik, E., "July 2010 7", Breaking and, <https://www.iis.se/docs/hjelmvik_breaking.pdf>.

[15] Vine, S., "Technology Showcase on Traffic Classification: Why Measurements and Freeform Policy Matter", May 2014, <https://www.sandvine.com/downloads/general/technology/sandvine-technology-showcases/sandvine-technology-showcase-traffic-classification.pdf#page=3>.

[16] Anonymous, A., "How to Bypass Comcast's Bittorrent Throttling", October 2007, <https://torrentfreak.com/how-to-bypass-comcast-bittorrent-throttling-071021>.

[17] Winter, P., "How China is Blocking Tor", April 2012, <http://arxiv.org/pdf/1204.0447v1.pdf21>.

[18] Anonymous, A., "GitHub blocked in China - how it happened, how to get around it, and where it will take us", January 2013, <https://en.greatfire.org/blog/2013/jan/github-blocked-china-how-it-happened-how-get-around-it-and-where-it-will-take-us>.

[19] Ensafi, R., "Detecting Intentional Packet Drops on the Internet via TCP/IP Side Channels", December 2013, <http://arxiv.org/pdf/1312.5739v1.pdf>.

[20] Aryan*, A., "Internet Censorship in Iran: A First Look", August 2013 , <https://jhalderm.com/pub/papers/iran-foci13.pdf>.

[21] Weaver, S., "Detecting Forged TCP Packets", June 2009 , <http://www.icir.org/vern/papers/reset-injection.ndss09.pdf>.

[22] Weaver, S., "Detecting Forged TCP Packets", June 2009 , <http://www.icir.org/vern/papers/reset-injection.ndss09.pdf>.

[23] Weaver, S., "Detecting Forged TCP Packets", June 2009 ,

<http://www.icir.org/vern/papers/reset-injection.ndss09.pdf>.

[24] Anonymous, A., "TCP-RST Injection", June 210 , <http://www.blackhatlibrary.net/TCP-RST_Injection >.

[25] Schoen, S., "EFF tests agree with AP: Comcast is forging packets to interfere with user traffic", October 19th,, <https://www.eff.org/deeplinks/2007/10/eff-tests-agree-ap-comcast-forging-packets-to-interfere>.

[26] VonLohmann, F., "FCC Rules Against Comcast for BitTorrent Blocking", August 3rd,, <https://www.eff.org/deeplinks/2008/08/fcc-rules-against-comcast-bit-torrent-blocking>.

[27] Phillip Winter, S., "How China Is Blocking Tor", April 2nd,, <http://arxiv.org/pdf/1204.0447v1.pdf#page=5>.

[28] DNS, V., "DNS Cache Poisoning in the People's Republic of China", September 6th, <http://viewdns.info/research/dns-cache-poisoning-in-the-peoples-republic-of-china/>.

[29] Aryan*, A., "Internet Censorship in Iran: A First Look", August 2013 , <https://jhalderm.com/pub/papers/iran-foci13.pdf#page=5>.

[30] Zmijewki, E., "Turkish Internet Censorship Takes a New Turn", March 2014, <http://www.renesys.com/2014/03/turkish-internet-censorship/>.

[31] Zmijewki, E., "Turkish Internet Censorship Takes a New Turn", March 2014, <http://www.renesys.com/2014/03/turkish-internet-censorship/>.

[32] AFP, ., "China Has Massive Internet Breakdown Reportedly Caused By Their Own Censoring Tools", January 2014, <http://www.businessinsider.com/chinas-internet-breakdown-reportedly-caused-by-censoring-tools-2014-1>.

[33] Anonymous, A., "The Collateral Damage of Internet Censorship by DNS Injection", July 2012 , <http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf>.

[34] Albert, K., "DNS Tampering and the new ICANN gTLD Rules", June 2011, <https://opennet.net/blog/2011/06/dns-tampering-and-new-icann-gtld-rules>.

[35] Anonymous, A., "Denial of Service Attacks (Wikipedia)"", N/A

N/A, <http://en.wikipedia.org/wiki/Denial-of-service_attack#Methods_of_attack>.

[36] Esposito, S., "Snowden Docs Show UK Spies Attacked Anonymous, Hackers", February 2014, <http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361>.

[37] CMU, ., "TCP SYN Flooding and IP Spoofing Attacks", November 2000, <http://www.cert.org/historical/advisories/CA-1996-21.cfm>.

[38] Villeneuve, N., "Open Access: Chapter 8, Control and Resistance, Attacks on Burmese Opposition Media", December 2011 , <http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-08.pdf>.

[39] Kravtsova, Y., "Cyberattacks Disrupt Opposition's Election", October 2012, <http://www.themoscowtimes.com/news/article/cyberattacks-disrupt-oppositions-election/470119.html>.

[40] Orion, E., "Zimbabwe election hit by hacking and DDoS attacks", August 2013, <http://www.theinquirer.net/inquirer/news/2287433/zimbabwe-election-hit-by-hacking-and-ddos-attacks>.

[41] Muncaster, P., "Malaysian election sparks web blocking/DDoS claims", May 2013, <http://www.theregister.co.uk/2013/05/09/malaysia_fraud_elections_ddos_web_blocking/>.

[42] Dobie, M., "Junta tightens media screw", September 2007, <http://news.bbc.co.uk/2/hi/asia-pacific/7016238.stm>.

[43] Heacock, R., "China Shuts Down Internet in Xinjiang Region After Riots", July 2009, <https://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots>.

[44] Cowie, J., "Egypt Leaves the Internet", January 2011, <http://www.renesys.com/2011/01/egypt-leaves-the-internet/>.

[45] Cowie, J., "Libyan Disconnect", February 2011, <http://www.renesys.com/2011/02/libyan-disconnect-1/>.

[46] Thomson, I., "Syria Cuts off Internet and Mobile Communication", November 2012, <http://www.theregister.co.uk/2012/11/29/syria_internet_blackout/>.

[47] News, B., "China employs two million microblog monitors state

media say", October 2013, <http://www.bbc.com/news/world-asia-china-24396957>.

[48] Calamur, K., "Prominent Egyptian Blogger Arrested", November 2013, <http://www.npr.org/blogs/thetwo-way/2013/11/29/247820503/prominent-egyptian-blogger-arrested>.

[49] Press, A., "Sattar Beheshit, Iranian Blogger, Was Beaten In Prison According To Prosecutor", December 2012, <http://www.huffingtonpost.com/2012/12/03/sattar-beheshit-iran_n_2233125.html>.

[50] Hopkins, C., "Communications Blocked in Libya, Qatari Blogger Arrested: This Week in Online Tyranny", March 2011, <http://readwrite.com/2011/03/03/communications_blocked_in_libya_this_week_in_onlin>.

[51] Gaurdian, T., "Chinese blogger jailed under crackdown on 'internet rumours'", April 2014, <http://www.theguardian.com/world/2014/apr/17/chinese-blogger-jailed-crackdown-internet-rumours-qin-zhihui>.

[52] Johnson, L., "Torture feared in arrest of Iraqi blogger", Febuary 2010, <http://seattlepostglobe.org/2010/02/05/torture-feared-in-arrest-of-iraqi-blogger/>.

[53] Bristow, M., "China's internet 'spin doctors'", November 2013, <http://news.bbc.co.uk/2/hi/asia-pacific/7783640.stm>.

[54] Fareed, M., "China joins a turf war", September 2008, <http://www.theguardian.com/media/2008/sep/22/chinathemedia.marketingandpr>.

[55] Gao, H., "Tiananmen, Forgotten", June 2014, <http://www.nytimes.com/2014/06/04/opinion/tiananmen-forgotten.html>.

[56] Anderson, R., "Access Denied: Tools and Technology of Internet Filtering", December 2011 , <http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-3.pdf#page=8>.

[57] Murdoch, S., "Access Denied: Tools and Technology of Internet Filtering", December 2011 , <http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-3.pdf#page=8>.

[58] Verkamp, J. and M. Gupta, "Inferring Mechanics of Web Censorship Around the World", August 2012, <https://www.usenix.org/system/files/conference/foci12/foci12-final1.pdf>.

[59] Nabi, Z., "The Anatomy of Web Censorship in Pakistan", August 2013, <http://0b4af6cdc2f0c5998459-c0245c5c937c5dedcca3f1764ecc9b2f.r43.cf2.rackcdn.com/12387-foci13-nabi.pdf>.

[60] Aryan, S., Aryan, H., and J. Halderman, "Internet Censorship in Iran: A First Look", August 2012, <http://0b4af6cdc2f0c5998459-c0245c5c937c5dedcca3f1764ecc9b2f.r43.cf2.rackcdn.com/12388-foci13-aryan.pdf>.

[61] Jones, B., "Automated Detection and Fingerprinting of Censorship Block Pages", November 2014, <http://conferences2.sigcomm.org/imc/2014/papers/p299.pdf>.

[62] Rushe, D., "Bing censoring Chinese language search results for users in the US", February 2015, <http://www.theguardian.com/technology/2014/feb/11/bing-censors-chinese-language-search-results>.

[63] Senft, A., "Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications", November 2013, <https://citizenlab.org/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/>.

[64] Clayton, R., "Ignoring the Great Firewall of China", January 2006, <http://link.springer.com/chapter/10.1007/11957454_2>.

[65] Anonymous, A., "Towards a Comprehensive Picture of the Great Firewall's DNS Censorship", August 2014, <https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf>.

[66] Khattak, S., "Towards Illuminating a Censorship Monitor's Model to Facilitate Evasion", August 2013, <http://0b4af6cdc2f0c5998459-c0245c5c937c5dedcca3f1764ecc9b2f.r43.cf2.rackcdn.com/12389-foci13-khattak.pdf>.

Authors' Addresses

Joseph L. Hall
CDT

Email: jhall@cdt.org

Michael D. Aaron
CU Boulder

Email: michael.aaron@colorado.edu

Ben Jones
GA Tech

Email: bjones99@gatech.edu